You Can't Protect What You Don't Know: The Future of Information Sharing

By Tim Meyers, Vice President, Federal Cybersecurity

Cybersecurity is about being one step ahead of attackers. But how is that possible without information?

One of the holes in the federal government's cybersecurity posture was the lack of a formal information sharing process between agencies. It's not unique to government, as the private sector has been battling its own issue with information sharing. However, the government has taken concrete steps recently to rectify the situation.

In March, President Joe Biden signed the Cyber Incident Reporting for Critical Infrastructure Act into law, which was included in an omnibus appropriations bill. With the specter of high-profile cyber-attacks on critical infrastructure and concern of retaliation in the wake of Russia's invasion of Ukraine, the House and Senate approved the legislation after similar bills had failed in recent years.

The legislation creates two new reporting obligations for critical infrastructure. First, certain cyber incidents must be reported to the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) within 72 hours. Second, any ransomware payments must be reported in a similar manner within 24 hours. The Act also expands the reporting obligations of covered entities and CISA's role with respect to cyber reporting initiatives, the rulemaking process, and information sharing among federal agencies.

While it's too early to evaluate how these obligations will change information sharing, it's a promising sign that we're moving in that direction. It's important because it will allow a broader viewpoint for all agencies to understand and identify all attack vectors.

One of the first laws in cybersecurity is that you need to know your assets. Simply put, you can't protect what you don't know about. Without insight into your assets and where attacks are coming from, cyber leaders are flying blind in terms of figuring out how to best protect their critical information from current and future attacks.

With information sharing, it becomes easier for agency leaders to respond in more effective ways. This information will help in putting the missing puzzle pieces together so the attack patterns are readily visible, and leaders can understand what is being targeted and the commonalities between attacks. If one agency, as an example, is under attack, that information being shared with other agencies that conduct similar business would be invaluable in preparing for and anticipating future attacks.

This is not a new concept, and we've seen information sharing become more prominent in industry, particularly on Wall Street. The Securities and Exchange Commission (SEC) passed a rule for investors that publicly traded companies have to share information about incidents

like ransomware, so other companies are aware and can prepare for similar attacks. The SEC did this because they want to protect the average investor, because they deserve to know if a company is being breached repeatedly and paying out ransoms.

As we look to the **future of cybersecurity**, there is consensus among experts that the rate and sophistication of attacks will only increase. We've already seen the impacts of the COVID-19 pandemic on cybersecurity, as more employees working from more remote locations opened up whole new avenues for cyber-attacks.

At a company like Maximus, where we handle tremendous amounts of sensitive or critical information on behalf of our federal clients, it's critical to continue making investments in our cyber practice. For example, Maximus has established a dedicated Cyber business unit that utilizes the latest, best practices and implements emerging technologies. Another example is achieving Cybersecurity Maturity Model Certification (CMMC), which serves as a verification mechanism to ensure the appropriate cybersecurity practices and processes are in place.

These investments are important for the private sector because it's necessary to provide new and emerging cyber capabilities to all federal agencies. There is no one-size-fits-all approach for cyber, so these capabilities need to span the full gamut of what agencies need. This includes building cyber programs, supporting cyber information sharing between agencies, engineering new cyber tools, and enabling world-class cyber operations by utilizing automation and orchestration techniques.

The cyber attacks are going to continue, there is no getting around that. Thus, it becomes incumbent on agency leaders to ensure their cyber policies are updated and prepared for anything that may come their way. Still, this process does not succeed without information.

The path forward for cybersecurity across federal agencies is lined by information sharing. Knowledge on previous attacks, including their origin and breadth, will allow all agencies to continuously update and modernize their cyber posture to prevent future attacks.

Cybersecurity is always a work in progress because the attackers are constantly improving and evolving their methods. Federal agencies need to be improving and evolving in response. Information sharing is vital to making that happen.